

# DEVICE AND METHOD FOR DATA INPUT/OUTPUT MANAGEMENT

**Publication number:** JP8087440 (A)

**Publication date:** 1996-04-02

**Inventor(s):** IMAI TORU; YOSHIDA HIDEKI; SEGAWA HIDEO

**Applicant(s):** TOKYO SHIBAURA ELECTRIC CO

**Classification:**

- international: **G06F12/14; G06F12/00; G06F21/24; G06F12/14; G06F12/00; G06F21/00;** (IPC1-7): G06F12/00; G06F12/14

- European:

**Application number:** JP19940221235 19940916

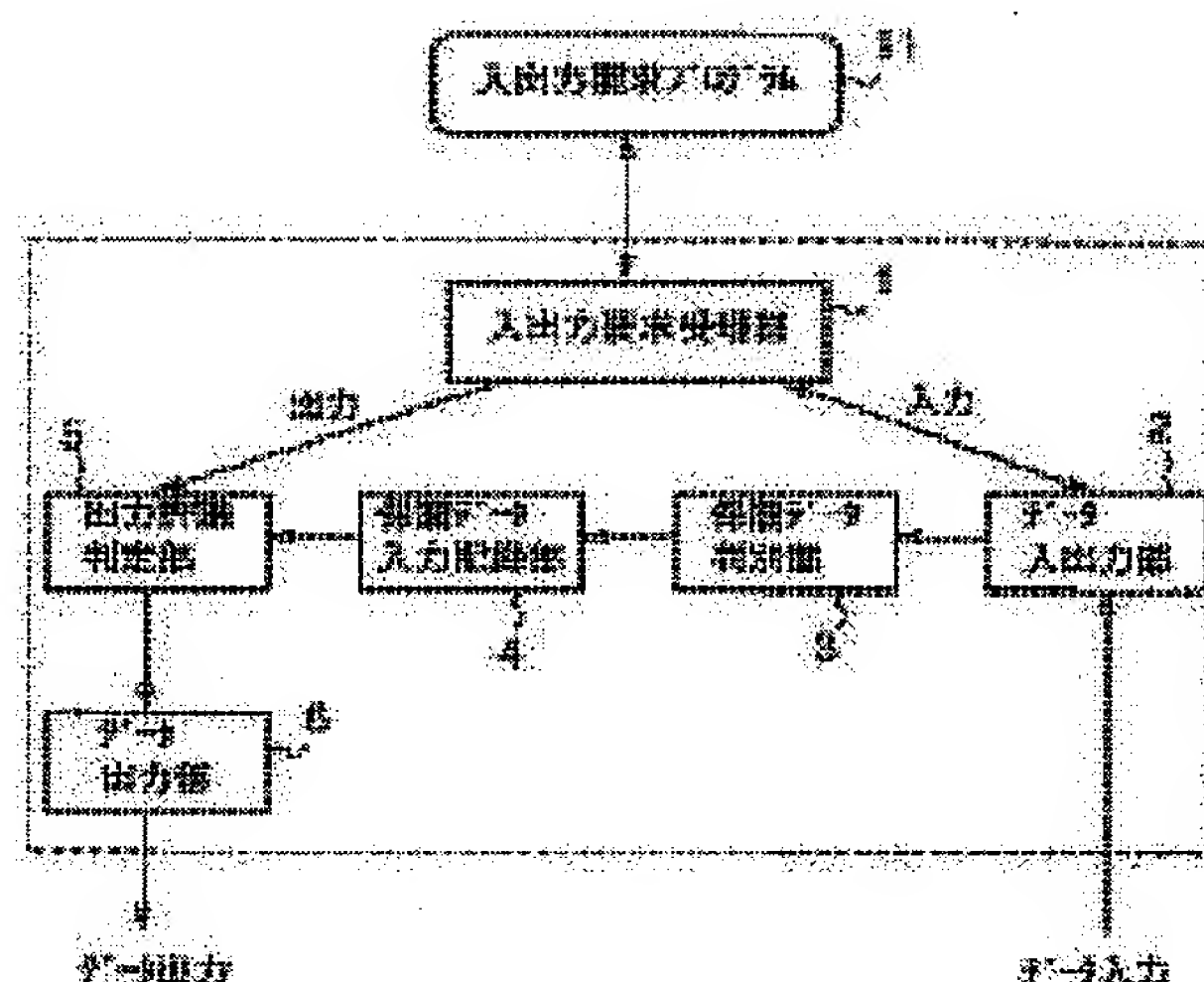
**Priority number(s):** JP19940221235 19940916

**Also published as:**

JP3637080 (B2)

## Abstract of JP 8087440 (A)

**PURPOSE:** To provide the data input/output management device which enables specified data to be read and displayed on a display device such as a display, but disables them to be copied and allows data other than the specified data to normally be outputted. **CONSTITUTION:** This device is equipped with a means 1 which accepts a data input/output request from a program together with the identifier of the program, a means 2 which inputs and supplies requested data to the program when the request is an input request, a means 3 which decides whether or not the inputted data are protected data, a means 4 which records at least the identifier of the program when the data are the protected data, a means 5 which allows the request unless the identifier of the program making the request is recorded when the request is an output request,; but determines whether or not the request is allowed on the basis of information showing an output-destination device making the request when the identifier is recorded, and a means 6 which outputs the requested data when the output request is accepted.



Data supplied from the esp@cenet database — Worldwide

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-87440

(43)公開日 平成8年(1996)4月2日

|                          |         |         |     |        |
|--------------------------|---------|---------|-----|--------|
| (51)Int.Cl. <sup>6</sup> | 識別記号    | 庁内整理番号  | F I | 技術表示箇所 |
| G 0 6 F 12/00            | 5 3 7 A | 7623-5B |     |        |
| 12/14                    | 3 2 0 E |         |     |        |

審査請求 未請求 請求項の数4 O L (全 13 頁)

(21)出願番号 特願平6-221235

(22)出願日 平成6年(1994)9月16日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 今井 徹

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 吉田 英樹

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 瀬川 英生

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

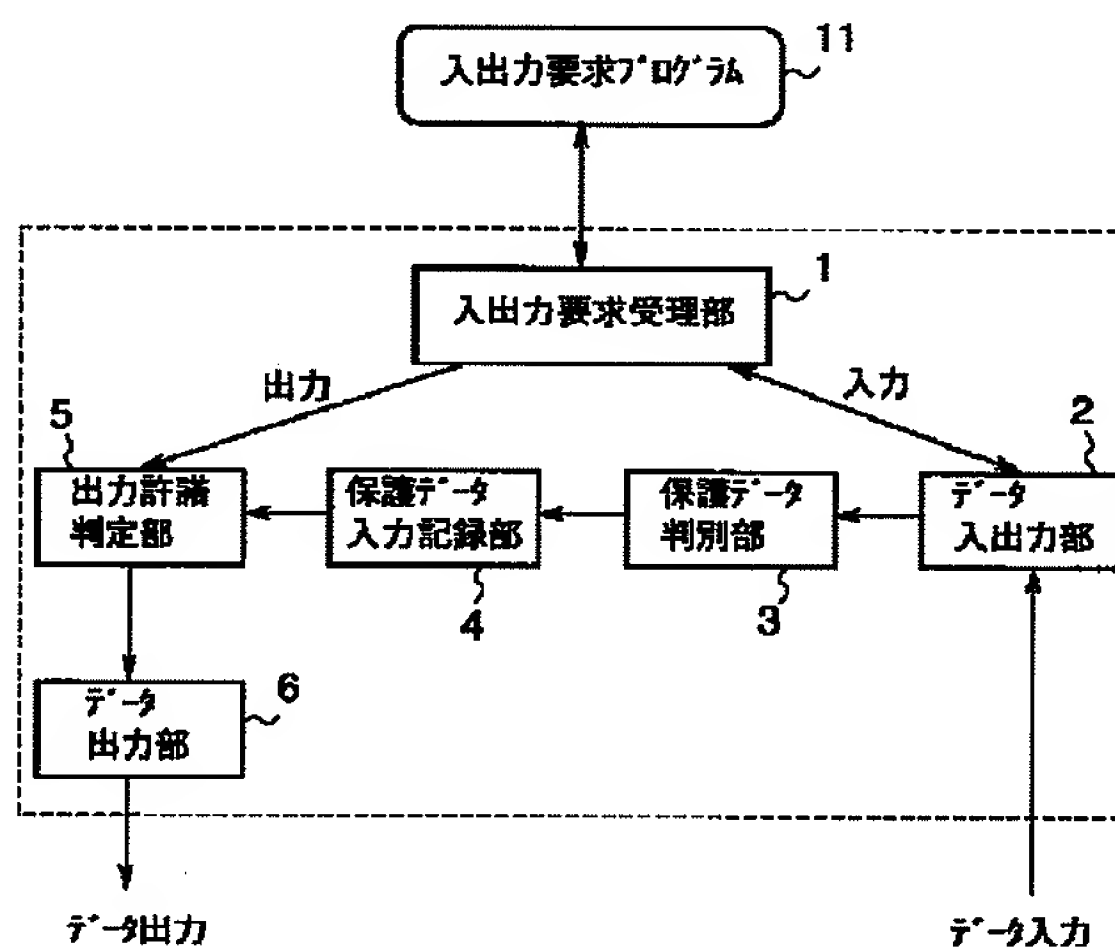
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 データ入出力管理装置及びデータ入出力管理方法

(57)【要約】

【目的】 指定されたデータに関して読むことやディスプレイ等の表示装置に表示することは可能であるが、複製することはできず、かつ指定されたデータ以外に関しては通常の出力を可能とするデータ入出力管理装置を提供すること。

【構成】 プログラムからのデータ入出力要求を該プログラムの識別子とともに受理する手段と、要求が入力要求である場合、要求のあったデータを入力しプログラムに与える手段と、入力されたデータが保護データであるか否かを判別する手段と、データが保護データである場合少なくともプログラムの識別子を記録する手段と、要求が出力要求である場合、要求を発したプログラムの識別子が記録されていないときは要求を承諾し、記録されていたときは少なくとも要求のあった出力先装置を示す情報に基づいて要求の諾否を決定する手段と、出力要求が承諾された場合、要求のあったデータを出力する手段を具備する。



## 【特許請求の範囲】

【請求項1】 プログラムから発せられたデータの入出力要求を該プログラムの識別子とともに受理する入出力要求受理手段と、

前記入出力要求が入力要求である場合、該入力要求のあったデータを入力し、前記プログラムに該データを与えるデータ入力手段と、

前記データ入力手段により入力された前記データが保護データであるか否かを判別する保護データ判別手段と、

前記データが保護データである場合、少なくとも前記プログラムの識別子を記録する保護データ入力記録手段と、

前記入出力要求が出力要求である場合、該出力要求を発した前記プログラムの識別子が前記保護データ入力記録手段に記録されていないときは該出力要求を許諾し、記録されていたときは少なくとも該出力要求のあった出力先装置を示す情報に基づいて出力要求の諾否を決定する出力許諾判定手段と、

この出力許諾判定手段により前記出力要求が許諾された場合、該出力要求のあったデータを出力するデータ出力手段を具備したことを特徴とするデータ入出力管理装置。

【請求項2】 前記プログラムは、新たな保護データの入力要求を発する場合、該保護データの入力を要求させるために、他のプログラムを新たに起動することを特徴とする請求項1に記載のデータ入出力管理装置。

【請求項3】 前記プログラムからの出力要求によらず前記プログラムの保持するデータを出力する機能を有する場合に、前記出力許諾手段は、データを出力しようとする該プログラムの識別子が前記保護データ入力記録手段に記録されていないときは、該プログラムのデータ出力を許諾し、記録されていたときは該プログラムのデータ出力を許諾しないことを特徴とする請求項1に記載のデータ入出力管理装置。

【請求項4】 プログラムから発せられたデータの入出力要求を該プログラムの識別子とともに受理するステップと、

前記入出力要求が入力要求である場合、該入力要求のあったデータを前記プログラムに与え、該データが保護データであるか否かを判別し、該データが保護データである場合、少なくとも前記プログラムの識別子を記録するステップと、

前記入出力要求が出力要求である場合、該出力要求を発した前記プログラムの識別子が前記保護データ入力記録手段に記録されていないときは該出力要求を許諾するとともに、記録されていたときは少なくとも該出力要求のあった出力先装置を示す情報に基づいて出力要求の諾否を決定し、該出力要求が許諾された場合、該出力要求のあったデータを出力するステップとを有することを特徴とするデータ入出力管理方法。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、プログラムからの入力要求に応じてデータを入力し、プログラムからの出力要求に応じてデータを出力するデータ入出力管理装置及びデータ入出力管理方法に関する。

## 【0002】

【従来の技術】 著作権を有する著作物の無断複製は、著作権法により禁じられている。しかしながら、著作物の無断複製を技術的に防ぐ手段が提供されていないため、それが行なわれるおそれがある。例えば、本、雑誌、新聞、データベースなどの著作物の全部または一部を複製することを技術的に防ぐことはできないため、法の規定に関わらず著作物の無断複製が行なわれるおそれがある。

【0003】 著作物が、ネットワーク、フロッピーディスク、CD-ROMなどの媒体を活用して電子的に提供される場合、さらに無断複製は深刻な問題となる。それは、紙で提供された著作物の複製は、コストや手間がかかる、品質が劣化する、任意の形式での表示ができないなどの欠点があるのに対して、電子的に提供された著作物の複製は、コストや手間は小さく、品質の劣化も小さく、さらにデジタル著作物の場合、任意の形式での表示や部分的な利用が可能であり、無断複製された著作物は元の著作物と比べ遜色がないからである。

【0004】 ところが、電子的な提供された著作物の無断複製を技術的に防ぐ手段は、従来の技術では備わっていない。例えば、著作物を計算機にロードして閲覧する場合、著作物を読み込みこれをユーザに提示するプログラムは、出力要求を発生することにより著作物を外部のポートや他のプロセス、ファイルなどに書き出すことができる。これは、一旦プログラムに著作物を与えたら、その著作物をどのように使用するかはプログラムに委ねられており、プログラムの動作を規定する手段が提供されていないためである。このため、著作物を電子的に形式のままの転載することが可能である。

【0005】 これを防ぐためには、例えばプログラムからのデータ出力要求をすべて拒絶すれば良いが、これではその計算機で動く全てのプログラムからのデータ出力が不可能になり、著作物アプリケーション以外のプログラムの動作に支障が生じる。また、ディスプレイのような媒体に著作物を表示する場合にもプログラムは出力要求を出すため、データ出力要求をすべて禁止すると著作物の表示ができないという問題が生じる。

【0006】 著作物に限らず、一般に、あるデータを読むことは許諾するが、データの複製やそのデータを基にしたデータの生成は禁止したい場合に、これを実現する手段が提供されていない。以下、読むことは可能であるが複製を禁じるデータを、「保護データ」と呼ぶ。プログラムに対して保護データが与えられると、このプログ

3

ラムは、読み込んだ保護データをファイルに書き込んだり、ポートから外部に出力したり、プロセス間通信により他のプログラムに与えることが可能であり、これにより保護データの複製を作られるおそれがある。

【0007】これを防ぐには、例えばすべての出力要求を拒絶すればよいが、これでは保護データを読んでいるプログラムからのデータ出力も不可能となり支障を生じる。また、出力要求を拒絶すると、複製を作成されるおそれのないディスプレイのような媒体への保護データの出力も禁止され、データ表示が全くできないという問題が生じる。

【0008】

【発明が解決しようとする課題】以上のように、従来のデータ入出力管理機構では、著作物データに対して画一的なアクセス制御しかできなかった。また、著作物データの出力を禁じたい場合、すべての出力装置に対するすべてのファイルの出力を禁じる形でしか実現できなかった。

【0009】したがって、従来のデータ入出力管理機構では、著作物データに対する読出し要求のみを許可する、あるいは複製されるおそれのないディスプレイのような媒体への出力のみ許可するといった、著作物データに対するきめ細かい管理を行うことができなかった。

【0010】本発明は、上記事情を考慮してなされたものであり、指定されたデータに関して読むことやディスプレイ等の表示装置に表示することは可能であるが、複製することはできず、かつ指定されたデータ以外に関しては通常の出力を可能とするデータ入出力管理装置及びデータ入出力管理方法を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明に係るデータ入出力管理装置は、プログラムから発せられたデータの出力要求を該プログラムの識別子とともに受理する入出力要求受理手段と、前記入出力要求が入力要求である場合、該入力要求のあったデータを入力し、前記プログラムに該データを与えるデータ入力手段と、前記データ入力手段により入力された前記データが保護データであるか否かを判別する保護データ判別手段と、前記データが保護データである場合、少なくとも前記プログラムの識別子を記録する保護データ入力記録手段と、前記入出力要求が出力要求である場合、該出力要求を発した前記プログラムの識別子が前記保護データ入力記録手段に記録されていないときは該出力要求を許諾し、記録されていたときは少なくとも該出力要求のあった出力先装置を示す情報に基づいて出力要求の諾否を決定する出力許諾判定手段と、この出力許諾判定手段により前記出力要求が許諾された場合、該出力要求のあったデータを出力するデータ出力手段を具備したことを特徴とする。

【0012】また、好ましくは、前記プログラムは、新たな保護データの出力要求を発する場合、該保護データ

4

の入力を要求させるために、他のプログラムを新たに起動しても良い。

【0013】また、好ましくは、前記出力許諾判定手段が、前記保護データ入力記録手段に記録される該プログラムに関する記録および出力先に応じて出力要求の諾否判定をすることを特徴とする。この場合、前記許諾出力先指定手段の指定に基づいて、前記出力許諾判定手段が出力要求の諾否判定をするようにしても良い。さらにこの場合、前記許諾出力先指定手段において、保護データの識別子ごとに許諾される出力先の指定ができるようにしても良い。

【0014】また、好ましくは、前記出力許諾判定手段が、前記出力要求に応じて保護データ入力記録手段の記録を変更することを特徴とする。また、好ましくは、前記プログラムからの出力要求によらず前記プログラムの保持するデータを出力する機能を有する場合に、前記出力許諾手段は、データを出力しようとする該プログラムの識別子が前記保護データ入力記録手段に記録されていないときは、該プログラムのデータ出力を許諾し、記録されていたときは該プログラムのデータ出力を許諾しないことを特徴とする。

【0015】本発明に係るデータ入出力管理方法は、プログラムから発せられたデータの出力要求を該プログラムの識別子とともに受理するステップと、前記入出力要求が入力要求である場合、該入力要求のあったデータを前記プログラムに与え、該データが保護データであるか否かを判別し、該データが保護データである場合、少なくとも前記プログラムの識別子を記録するステップと、前記入出力要求が出力要求である場合、該出力要求を発した前記プログラムの識別子が前記保護データ入力記録手段に記録されていないときは該出力要求を許諾するとともに、記録されていたときは少なくとも該出力要求のあった出力先装置を示す情報に基づいて出力要求の諾否を決定し、該出力要求が許諾された場合、該出力要求のあったデータを出力するステップとを有することを特徴とする。

【0016】

【作用】本発明では、プログラムからデータの出力要求が発せられた時、入出力要求受理手段にてこれを受理し、入力要求である場合にデータ入力手段にてデータを読み出し、保護データ判別手段によりこのデータが保護データであるか否かを判別し、保護データであれば保護データ入力記録手段に該プログラムが保護データを入力したことを記録する。

【0017】これによって、各プログラムが保護データを読んだか否かを管理することができる。プログラムから入出力要求が出力要求である場合、該プログラムが保護データを読んでいるいなければ、出力要求を許諾すれば良い。保護データを読んでいるいれば、それがディスプレイのような他のプログラムから読むことのできない対象であ



れば許諾し、さもなければ拒否する。

【0018】許諾されたデータは、データ出力手段により出力される。これによって、保護データを読んでいるプログラムについては、通常の出力量が許諾され、読んだプログラムについては、複製の可能性がない場合のみ出力量が許諾される。

【0019】従って、本発明によれば、保護データは読むことは可能であるが複製することはできず、ディスプレイ等の表示装置には表示することが可能であり、かつ保護データ以外は通常の出力量を可能とすることができる。

【0020】

【実施例】以下、図面を参照しながら本発明の実施例を説明する。図1は、本発明の実施例に係るデータ入出力管理装置の概略構成図である。図1のように、本実施例のデータ入出力管理装置は、入出力要求受理部1、データ入力部2、保護データ判別部3、保護データ入力記録部4、出力許諾判定部5、データ出力部6からなる。

【0021】図2は、本実施例の動作を示すフローチャートである。入出力要求プログラム11が要求を発生すると、入出力要求受理部1はこの要求を受理し、入出力要求プログラム11の識別子および要求の種類を判別する(ステップS21)。

【0022】通常、OS内部にはプロセスからのシステムコールを受け取りシステムコールの種類を判別するプログラムが提供されているが、上記の入出力要求受理部1はこれに相当するものである。入出力要求プログラム11は、入出力要求受理部1と同じ計算機にて実行されていても、別の計算機にて実行されていても良い。例えば、同じ計算機にて実行されている場合は、プロセスIDを識別子とすればよく、別の計算機にて実行されている場合は、ホストIDとプロセスIDの対を識別子とすればよい。要求の種類の受渡しは、要求を発する際に特定のレジスタに要求の識別子を書き込む、あるいは要求の先頭で識別子を送るなど、あらかじめ定めた手続きによって入出力要求プログラム11が指定し、これを入出力要求受理部1が読み出して判別すれば良い(ステップS22)。

【0023】入出力要求受理部1により入力要求であることがわかると、データ入力部2が要求されているデータを入力する(ステップS23)。データ入力部2は、該データがディスク、CD-ROM、テープなどの記憶媒体に記憶されているなら、ここから読み出す。また、ネットワークのような蓄積型でない媒体からデータを読んできて良い。OSにおけるデバイスドライバと呼ばれるソフトが、これらに相当する。

【0024】保護データ判別部3は、入力を要求されたデータが保護データであるか否かを判別する(ステップS24)。本実施例では、読み込まれるデータは記憶媒体にファイルとして記憶されており、保護データを含む

ファイルはあらかじめ定められた形式のヘッダを有しているものとする。従って、保護データ判別部3は読み込んだファイルが本形式のヘッダを有していれば保護データであり、そうでなければ保護データではないと判別すれば良い。このヘッダの形式は、あらかじめ保護データ判別部3に記録されていても良いし、別のファイルに記録されていて保護データ判別部3がそのファイルを参照して知っても良い。また、別のプログラムが管理し、保護データ判別部3に通知しても良い。

【0025】また、別の判別方法をとってもよい。例えば、ファイル自体に保護データを格納しているか否かを判別するための情報が付加してあるのではなく、データが格納されるファイルの名前により保護データかそうでないかが決定される、あるいはファイルの記憶される媒体の種類、記憶媒体の中の記憶位置により決定されるなどの方式でも良い。

【0026】図3は、保護データを含むファイルが有しているヘッダの例を示す図である。本実施例では、保護データを格納するファイルには、定まった形式のヘッダが付加されているものとする。このヘッダを所有するファイルに格納されているデータは保護データであり、所有していないファイルに格納されているデータは保護データではない。ヘッダには、保護データを含むファイルであることを示す番号、データファイルを示すデータファイルID、製作者を示す製作者ID、暗号化された保護データを復号するための鍵を特定するための復号鍵番号、などが記述されている。

【0027】次に、判別の結果、保護データを含むものであった場合は、保護データ入力記録部4に記録を行う(ステップS25)。図4は、本実施例の保護データ入力記録部4の構造の一例を示す図である。該データが保護データであると判別されたら、保護データ入力記録部4に、入出力要求プログラム11の識別子を記録する。すでに当該識別子が記録されていれば、記録しなくてもよい。本実施例では、本保護データ入出力管理方式から少なくとも一つの保護データを読んだプロセスのIDがリスト構造として記録されている。

【0028】例えば図4では、図中21のポインタが示すリスト(図中の22)に、プロセスID(図中の23)である“5”と次のリンク先へのポインタ(図中の24)が格納されている。リンク先がない場合は、そのことを示すデータを格納する(図中の25)。

【0029】最後に、入出力要求プログラム11にデータを与える(ステップS26)。データが暗号化されていた場合、これを復号して渡しても良い。このためには、ヘッダに記載されている復号鍵の番号と暗号化されたデータを復号化部に渡す。これは、ソフトウェアにより実現しても、セキュリティを高めるためにハードウェアにより実現しても良い。入出力要求プログラム11が別の計算機にて動作している場合は、復号鍵と共に暗号

7

化されたデータを与え、入出力要求プログラム 11 が動作している計算機にて復号しても良い。

【0030】一方、入出力要求プログラム 11 が出力要求を発生すると、入出力要求受理部 1 が出力要求であることを検出する(ステップ S 22)。出力許諾判定部 5 は、該出力要求を発生した入出力要求プログラム 11 の識別子が保護データ入力記録部 4 に記録されているかどうかを調べる(ステップ S 27)。

【0031】記録されていなければ、該入出力要求プログラム 11 は保護データを読んでいないから、保護データを出力する可能性はない。このため出力要求を許諾して良い(ステップ S 28)。

【0032】これに対し、入出力要求プログラム 11 の識別子が保護データ入力記録部 4 に記録されていれば、該入出力要求プログラム 11 は保護データを読んだプログラムであるから、出力要求先によって出力要求を認めるかそうでないかを判断する(ステップ S 29)。

【0033】出力先が別のプログラムあるいはディスプレイのような他のプログラムから直接はデータを読めない出力機器であれば、出力要求を許諾して良い(ステップ S 30)。

【0034】さもなければ、保護データが複製されるおそれがあるので、出力は拒否される(ステップ S 31)。出力要求が許可される(ステップ S 28, S 30)と、データ出力部 6 により出力が行われる(ステップ S 32)。

【0035】従って、保護データを読んだことのないプログラムからは自由にデータの出力ができ、保護データを読んだプログラムからの出力はディスプレイのような恒久的でない対象にのみ許し、他への出力は禁じることができる。これにより、保護データが複製されるおそれがなく、あるいは保護データを読んだことのないプログラムからは自由にデータの出力ができる入出データ力管理方式が実現できる。

【0036】(第 2 の実施例) 第 1 の実施例では、出力許諾判定部 5 は、入出力要求プログラム 11 の識別子が保護データ入力記録部 4 に記録されている場合、出力先がディスプレイであるかどうかを判別して出力を諾否を判定している。しかし、出力先は固定されない方が良い場合もある。例えば、一つの計算機が複数のディスプレイを所持している場合、すべてのディスプレイに出力したいとは限らない。また、ディスプレイ以外の特定の機器に保護データの出力をしたい場合もある。このような保護データの出力が許諾される出力先の変更を可能とするためには、保護データの許諾出力先を許諾出力先指定部 7 にて指定できるようにすればよい。第 2 の実施例では、これを実現するための一例を示す。

【0037】図 5 は、第 2 の実施例のデータ入出力管理装置の概略構成図である。本実施例においては、第 1 の実施例の構成に許諾出力先指定部 7 が加わり、出力許諾

8

判定部 5 は、保護データ入力記録部 4 および許諾出力先指定部 7 を参照するところが第 1 の実施例と異なる。

【0038】図 6 は、本実施例の許諾出力先指定部 7 の一例である。これによって、保護データの出力が許諾される出力先のテーブルが与えられる。出力許諾判定部 5 は、出力要求先がこのリストに含まれるなら出力を許諾し、含まれなければ拒絶する。本実施例では、“/dev/console”のように OS が管理するデバイスの仮想的な名前で指定したが、これに限定されず、ポート番号など一意に出力先が特定できる識別子として出力先を指定すれば良い。本出力先テーブルは、不当に変更されると保護データの複製のおそれがあるので、OS が管理する等の方法で高いセキュリティを保つ必要がある。

【0039】以上のように、本実施例によれば、保護データの出力が許諾される出力先を変更することも可能となる。

(第 3 の実施例) 第 2 の実施例では、全ての保護データに関して出力可能な出力先は共通である。しかし、ある保護データはある出力先に出力したいが、別の保護データはその出力先には出力できないようにしたいような場合もある。この場合には、許諾出力先指定部 7 に保護データ毎の許諾出力先を指定しておくと共に、保護データ入力記録部 4 にて各プログラムに与えられた保護データの識別子を記録しておき、出力許諾判定部 5 はこれらを参照して出力許諾を判定すれば良い。第 3 の実施例では、これを実現するための一例を示す。

【0040】図 7 は、本実施例の保護データ入力記録部 4 の構造の一例を示す図である。該データが保護データであると判別されたら、保護データ入力記録部 4 に、入出力要求プログラム 11 の識別子を記録する。すでに該入出力要求プログラム 11 の識別子が記録されていれば、その入出力要求プログラム 11 の読んだ保護データのリストに該データファイル ID を記録する。該入出力要求プログラム 11 の識別子が記録されていなければ、新たに記録し、その入出力要求プログラム 11 の読んだ保護データとして該データファイル ID を記録する。

【0041】例えば図 7 では、図中 31 のポインタが示すリスト(図中の 32)に、プロセス ID(図中の 33)である“5”、データファイル ID のリストのリンク先へのポインタ(図中の 34)、次のプロセス ID のリストのリンク先へのポインタ(図中の 35)が格納されている。図中 36 のリストには、データファイル ID(図中の 37)である“123”、次のリンク先へのポインタ(図中の 38)が格納されている。同様にして、図 7 では、データファイル ID が 5、20、25、40 のプロセスが保護データを読んだプログラムとしてリスト構造として記録されており、さらに ID 5 のプロセスは、データファイル ID が 123 と 25 の 2 種類の保護データを読んでおり、ID 20 のプロセスは、データフ

ファイルIDが8の保護データを、ID25のプロセスは、データファイルIDが123の保護データを、ID40のプロセスは、データファイルIDが85の保護データを読んでいることがわかる。なお、リンク先がない場合は、そのことを示すデータを格納する(図中の39, 40)。

【0042】図8は、本実施例の許諾出力先指定部7の一例である。これは、出力先とそれへの出力が許諾されるデータファイルIDの対応表である。第1行目は、すべてのデータファイルが、“/dev/console”に出力可能であることを示す。第2行目は、データファイルIDが123か65であれば、“/dev/tty0”に出力可能であることを示す。第3行目は、データファイルIDが0以上127以下であるものは、“/dev/fb”に出力可能であることを示す。第4行目は、データファイルIDが0以上127以下でないものは、“/dev/win1”に出力可能であることを示す。

【0043】出力許諾判定部5は、入出力要求プログラム11の識別子から保護データ入力記録部4を検索し、そのプログラムが読んだデータファイルIDを得る。一つのデータファイルしか記録されていない場合は、許諾出力先指定部7を検索し、そのデータファイルは要求された出力先に出力することが許諾されているか否かを調べる。例えば、“プロセス20”から、“/dev/fb”に出力要求があった場合、出力許諾判定部5は次の処理を行なう。まず、保護データ入力記録部4を検索し、“プロセス20”は“データファイル8”を読んでいることがわかる。次に、許諾出力先指定部7を検索すると、“データファイル8”は、“/dev/fb”への出力が許諾されている。従って“プロセス20”から、“/dev/fb”への出力要求は許諾して良い。

【0044】出力許諾判定部5が、入出力要求プログラム11の識別子から保護データ入力記録部4を検索し、そのプログラムが読んだデータファイルが2つ以上ある場合、許諾出力先指定部7を検索するが、これらすべてのデータファイルの要求出力先への出力が許諾されている場合のみ、出力を許諾する。例えば、“プロセス5”から、“/dev/tty0”に出力要求があった場合、出力許諾判定部5は次の処理を行なう。まず、保護データ入力記録部4を検索し、“プロセス5”は“データファイル123”と“データファイル25”を読んでいることがわかる。次に、許諾出力先指定部7を検索すると、“データファイル123”は、“/dev/tty0”への出力が許諾されているが、“データファイル25”は、“/dev/tty0”への出力が許諾されていない。従って、もし出力を許諾すると、“データファイル25”が格納する保護データが禁じられている出力先に出力されるおそれがある。よって、出力許諾判定部5は、“プロセス5”からの“/dev/tty0”

への出力要求は拒絶する。

【0045】以上のように、本実施例によれば、保護データごとに出力が許諾される出力先が指定でき、許諾された以外の出力先には出力できないようにすることが可能となる。

【0046】(第4の実施例) 第1の実施例では、保護データはプログラムからの入力要求によってしか起こらないものとしたが、第2の実施例では、プログラム間で通信を行ないデータの授受を行なう機能をOSが有している場合のデータ入出力管理方式を取り上げる。プログラム間でデータの授受を行なう機能を有するOSにおいてプログラムが実行されている場合、保護データを読んだプログラムが他のプログラムにデータを渡すことができる。このため、プログラム間での通信も管理しなければならない。

【0047】図9は、第4の実施例のデータ入出力管理装置の概略構成図である。本実施例においては、出力許諾判定部5は、保護データ入力記録部4の記録を参照するだけでなく、変更もする点が、第1の実施例と異なる。

【0048】図10は、本実施例の動作を示すフローチャートである。このフローチャートは、図2のフローチャートと大部分が同様のものであり、図2のステップS31の処理内容を変更したものである。ここでは、図2のフローチャートと異なる部分だけ説明する。

【0049】保護データを読んだプログラムが出力要求を行ない(ステップS22, ステップS27)、その出力先がディスプレイのような他のプログラムがデータを読み出すことができない対象でない場合(ステップS29)、出力許諾判定部5は、出力先が他のプログラムであるかどうかを調べる(ステップS41)。

【0050】もしそうであれば、出力先のプログラムも保護データを受けとる可能性があるため、出力先プログラムの識別子が保護データ入力記録部4に記録されていなければこれを記録する(ステップS42)。そして、データ出力部6によりプログラム間でのデータの授受を行なえば良い(ステップS32)。

【0051】ステップS41にて、もし出力先は他のプログラムでなければ、出力は拒否される(ステップS43)。従って、保護データを読んでいるプログラムからは、従来通りに自由にデータの転送ができる。保護データを読んだプログラムからは、ディスプレイのような他のプログラムからはデータを読み出すことのできない対象にはデータの出力ができ、他のプログラムに対してはデータの授受ができるが、受けとったプログラムも以降では保護データを読んだプログラムとして扱われる。それ以外の対象には、データは出力されない。これにより、保護データの複製が防止できる。

【0052】(第5の実施例) 第1の実施例や第4の実施例では、保護データを読んでいるプログラムからの



出力要求は許諾し、保護データを読んだプログラムからの出力要求は保護データの複製が起こらないような状況でのみ許諾した。したがって、保護データを読んだプログラムからは、たとえ保護データではないデータであってもファイルや外部ポートのような対象に出力することは拒否される。

【0053】本実施例では、プログラムから出力要求が発せられた時、その出力データが保護データに起因するものであるかそうでないかによって、異なった出力制御ができるようにしたものである。これによって、例えばアプリケーションプログラムが保護データを読んでユーザに表示し、ユーザはそれに関連するメモを作成したいときにメモを保存することができるようになるなど、実用上多大なる効果がある。

【0054】第5の実施例は、プログラムは保護データを読み込むこともでき、かつ保護データに起因しないデータをファイルや外部ポートのような対象に出力することができるようにしたものである。

【0055】図11は、第5の実施例の概略構成図である。まず、保護データを読んでいないプログラム1（図中の11）が保護データの入力を要求する時、まずプログラム2（図中の12）を生成する。

【0056】例えば、UNIXでは、forkというシステムコールによりプログラム1を実行しているプロセスの複製を作成してプログラム2と考えれば良い。他のOSにおいても、新たなプロセスやタスクの生成をOSに対して要求すれば良い。

【0057】次に、プログラム2から保護データ入出力要求が発生する。この要求は入出力要求受理部1にて受理され、第1の実施例や第4の実施例と同様に、保護データ入力記録部4に、プログラム2に保護データが与えられたことが記録され、プログラム2は保護データを読むことができる。

【0058】プログラム2からデータ出力要求が発生された場合には、第1の実施例や第2の実施例と同様に処理され、ファイルや外部ポートのような対象にデータを出力することはできない。

【0059】しかしながら、プログラム1からデータ出力要求が発生された場合は、プログラム1は保護データを読んでいないため、対象にかかわらずデータを出力することができる。従って、ファイルや外部ポートのような対象に出力したい保護する必要のないデータは、プログラム1が所持することにすれば、自由に出力することができる。

【0060】これは、例えば次のようにすれば実現できる。まず、プログラム1は、保護データを読んでいない状態で実行を開始する。保護データの入力を行なう際は、新たなプログラム2を生成し、このプログラム2に入力要求が発生させる。ユーザからの入力や保護データ以外のデータの入力は、保護データを入力していないプ

ログラム1が行なう。これによって、保護データと保護されていないデータを別のプログラムに分離して管理することができる。従って、保護されていないデータは、ファイルや外部ポートのような対象に出力することができる。

【0061】ここで、保護データを2回以上読み込む時は、次の3通りの方式が考えられる。

- ・以前に保護データを読んだプログラム2が保護データを読む方式

- ・以前に保護データを読んだプログラム2やプログラム1とは別の第3のプログラムが保護データを読む方式

- ・以前に読んだ保護データとヘッダの内容が等価な保護データを読む時は、以前に保護データを読んだプログラム2が読み、さもなければ新たな第3のプログラムが保護データを読む方式

いずれの方式においても、保護されてなくファイルや外部ポートのような対象に出力する可能性のあるデータを所有するプログラムと、保護データを所有するプログラムが分離されていれば良い。

【0062】（第6の実施例）第1～第5の実施例では、該プログラムからの出力要求時にデータ出力の許諾判定を行う実施例を示した。ところが、該プログラムの所持するデータを該プログラムからの出力要求なしに出力する機能をデータ入出力管理装置が有している場合もある。

【0063】例えば、計算機システムにおいて、実際に存在する物理メモリの量を上回るプログラムを実行するために、現在実行が停止されているプログラムのテキストやデータはディスクなどの二次記憶に退避し、必要になったときにメモリにロードする手法がとられていることがある。これらは、ページングやスワッピングと呼ばれる手法であるが、該プログラムからの出力要求がないにもかかわらず、該プログラムのデータが二次記憶に退避される。こういった機能を有する場合に、保護データが二次記憶に退避されたところで二次記憶媒体を取り外し、他の計算機につなぎ読み出すことにより、メモリ上に展開されていた保護データを複写されるという問題がある。これを防ぐためには、保護データがロードされているメモリ上の領域は二次記憶に退避しないようにすれば良い。

【0064】該プログラムの所持するデータが該プログラムからの出力要求なしに出力される別の例として、次のような場合がある。プログラムの開発を支援するために、異常事態が起こったときにプログラムのデータをファイルに複写する機能を提供する計算機システムがある。この機能は、例えばUNIXではコアダンプと呼ばれる。コアダンプは、プログラムのデータをファイルに記録するため、これを読み出すことにより元のデータを再生することが可能である。

【0065】図12は、第6の実施例のデータ入出力管



13

理装置の概略構成図である。本実施例においては、データ入出力管理装置が、データ出力要求部17を有する。データ出力要求部17は、上で述べた二次記憶への退避、コアダンプの作成などの目的に、プログラムの識別子とデータ出力範囲を指定してデータ出力を要求する。出力許諾判定部5は、データ出力要求部17からの出力要求を受けると、図2のステップS27に記した入力要求受理部1からの要求を受けた場合と同様に、保護データ入力記憶部4を参照し、該プログラムが記録されているかどうかを調べる。記録されていないならば、該プログラムは保護データを読んでいないから、出力を許諾しても保護データが出力される可能性はない。このため出力要求を許諾して良い。これに対し、該プログラムの識別子が保護データ入力記憶部4に記録されていれば、該プログラムは保護データを読んだプログラムであるから、図2のステップS29と同様に出力要求先によって出力要求を認めるかそうでないかを判断する。出力先が別のプログラムあるいはディスプレイのような他のプログラムから直接はデータを読めない出力機器であれば、出力要求を許諾して良い(図2のステップS30)。さもなければ、保護データが複製されるおそれがあるので、出力は拒否される(図2のステップS31)。出力要求が許可されると、データ出力部6により出力される(図2のステップS32)。なお、入出力プログラム11から入出力要求があったときの1から6の動作は、第1の実施例で述べたものと同等である。

【0066】以上のように、該プログラムの所持するデータを該プログラムからの出力要求なしに出力する機能をデータ入出力管理装置が有している場合でも、保護データを読んだことのないプログラムからは自由にデータの出力ができ、保護データを読んだことのないプログラムからの出力はディスプレイのような恒久的でない対象にのみ許し、他への出力は禁じることができる。これにより、保護データが複製するおそれがなく、かつ保護データを読んだことのないプログラムからは自由にデータの出力ができる入出力データ管理方式が実現できる。

【0067】また、出力要求は、明示的にデータを書き出す要求だけに限定されない。例えば、UNIXのシステムコール「fork」のように、プログラムの複製を作る要求が発生されると、元のプログラムデータ部に複製される。この場合も、データが別のプログラムに出力されるわけであるから、出力要求に含まれるものと解釈する。

14

【0068】また、ファイルの属性(名前、モード、時刻など)を変えるような要求も、ファイルシステムに対し、新たに設定する属性を出力する要求であるので、出力要求に含まれるものと解釈する。

【0069】なお、ここで取り上げた実施例ではプロセスからの要求は要求受理部1で一括して扱ったが、入力要求を受理する入力要求受理部1と出力要求を受理する出力要求受理部1とに独立させれば、それぞれは図2や図10のステップS22のような要求の種類を判別する機能は持たなくても良い。なお、本発明は上述した各実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【0070】

【発明の効果】以上説明したように、本発明によれば、各プログラムが保護データを読んだか否かを管理するとともに、プログラムから出力要求を受けた場合、該プログラムが保護データを読んだか否かを調べ、および読んだものであるときには出力先装置を調べた上で、出力要求の諾否を決定するようにしたので、指定されたデータに関して、読むことは可能であるが複製することはできず、ディスプレイ等の表示装置に表示することが可能であり、かつ指定された以外のデータに関しては通常の出力を可能とすることができる。

【図面の簡単な説明】

【図1】第1の実施例の概略構成を示す図

【図2】第1の実施例の動作を示すフローチャート

【図3】保護データを含むファイルに付加されるヘッダの例を示す図

【図4】保護データ入力記録部4の例を示す図

【図5】第2の実施例の概略構成を示す図

【図6】許諾出力先指定部の一例を示す図

【図7】第3の実施例の保護データ入力記録部の一例を示す図

【図8】許諾出力先指定部の一例を示す図

【図9】第4の実施例の概略構成を示す図

【図10】第4の実施例の動作を示すフローチャート

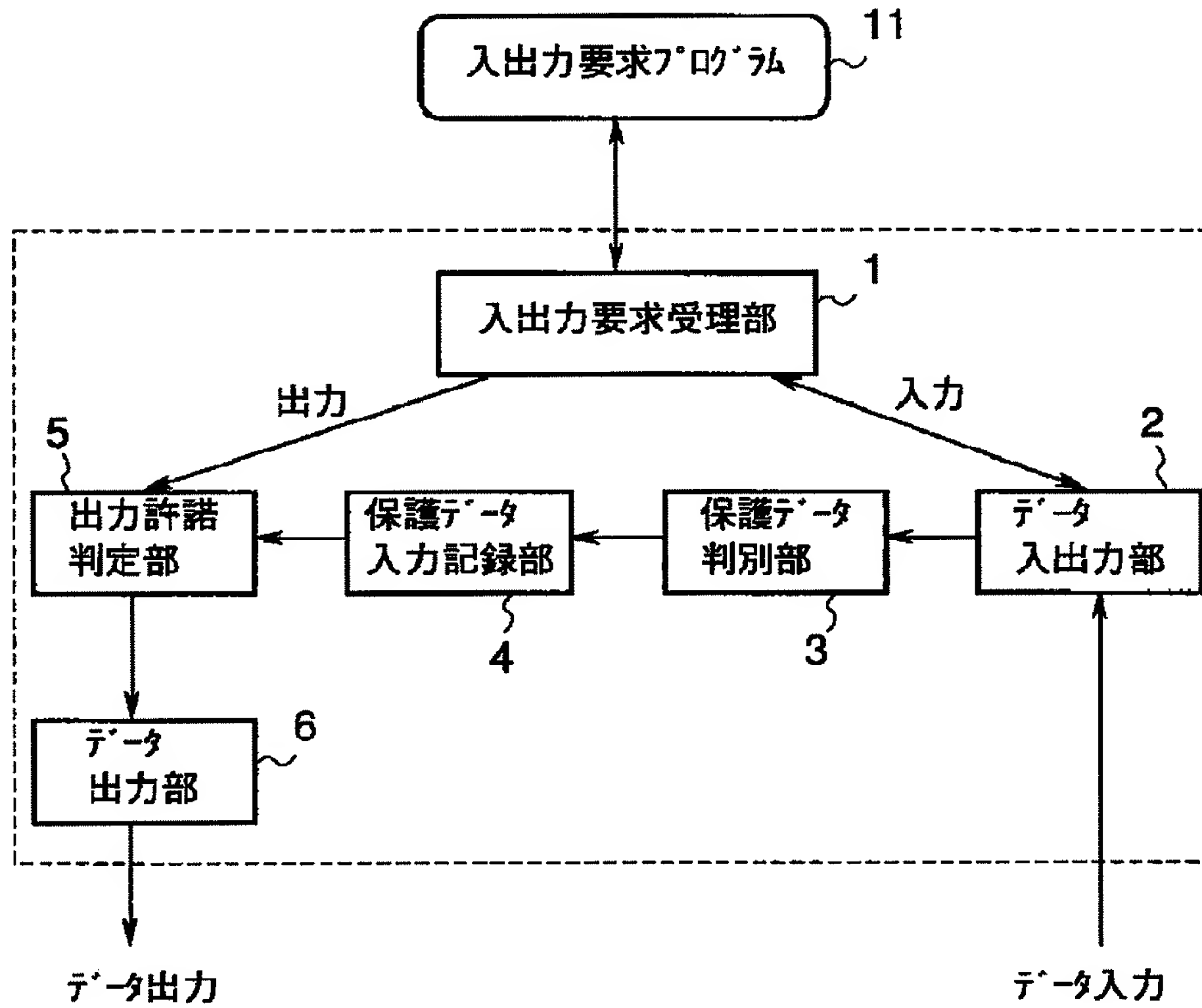
【図11】第5の実施例の概略構成を示す図

【図12】第6の実施例の概略構成を示す図

【符号の説明】

1…入出力要求受理部、2…データ入力部、3…保護データ判別部、4…保護データ入力記録部、5…出力許諾判定部、6…データ出力部、7…許諾出力先指定部、17…データ出力要求部

【図1】



【図6】

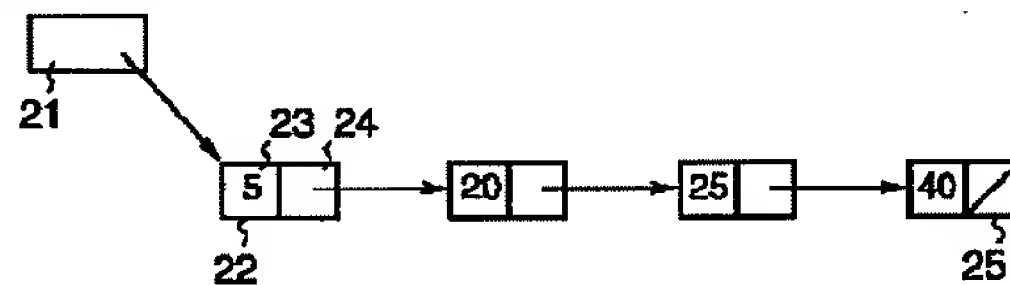
| 許諾される出力先     |
|--------------|
| /dev/console |
| /dev/ttyφ    |
| /dev/fb      |
| /dev/win 1   |
| ⋮            |

【図3】

| 〈保護データファイルであることを示す番号〉 |      |
|-----------------------|------|
| データファイルID             | 4567 |
| 製作者ID                 | 123  |
| 複号鍵番号                 | 28   |
| ⋮                     | ⋮    |

【図4】

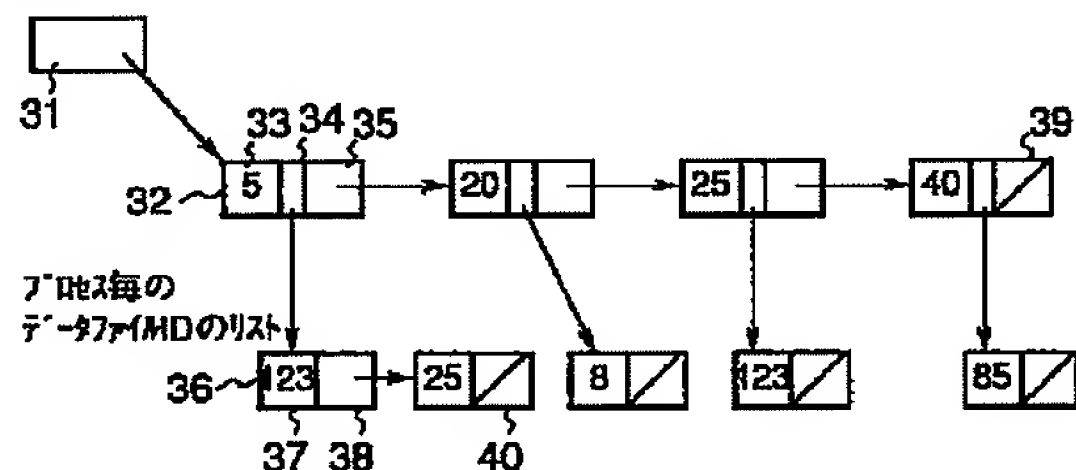
保護データを入力したアドレスリスト



【図8】

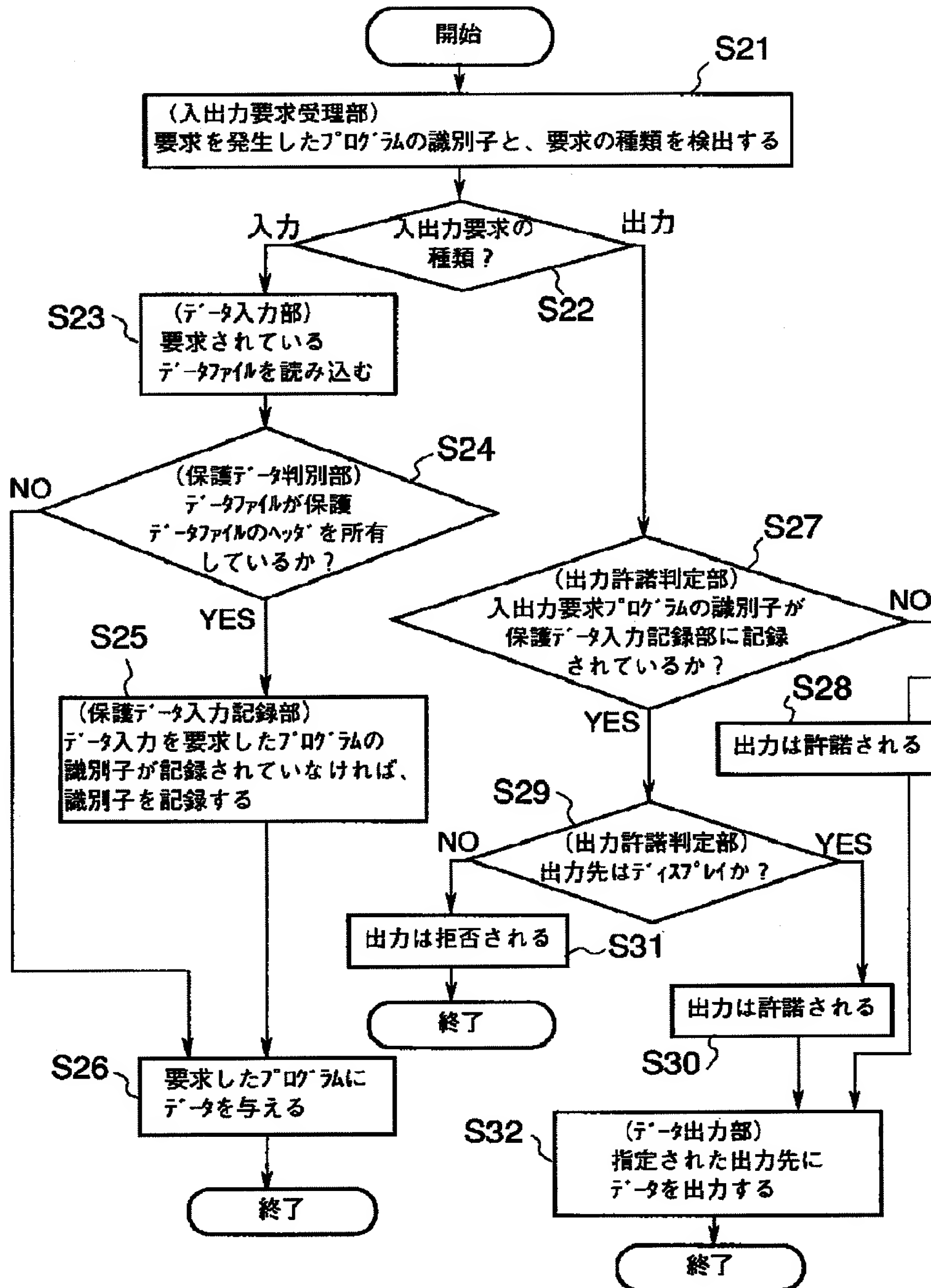
【図7】

保護データを入力したアドレスリスト



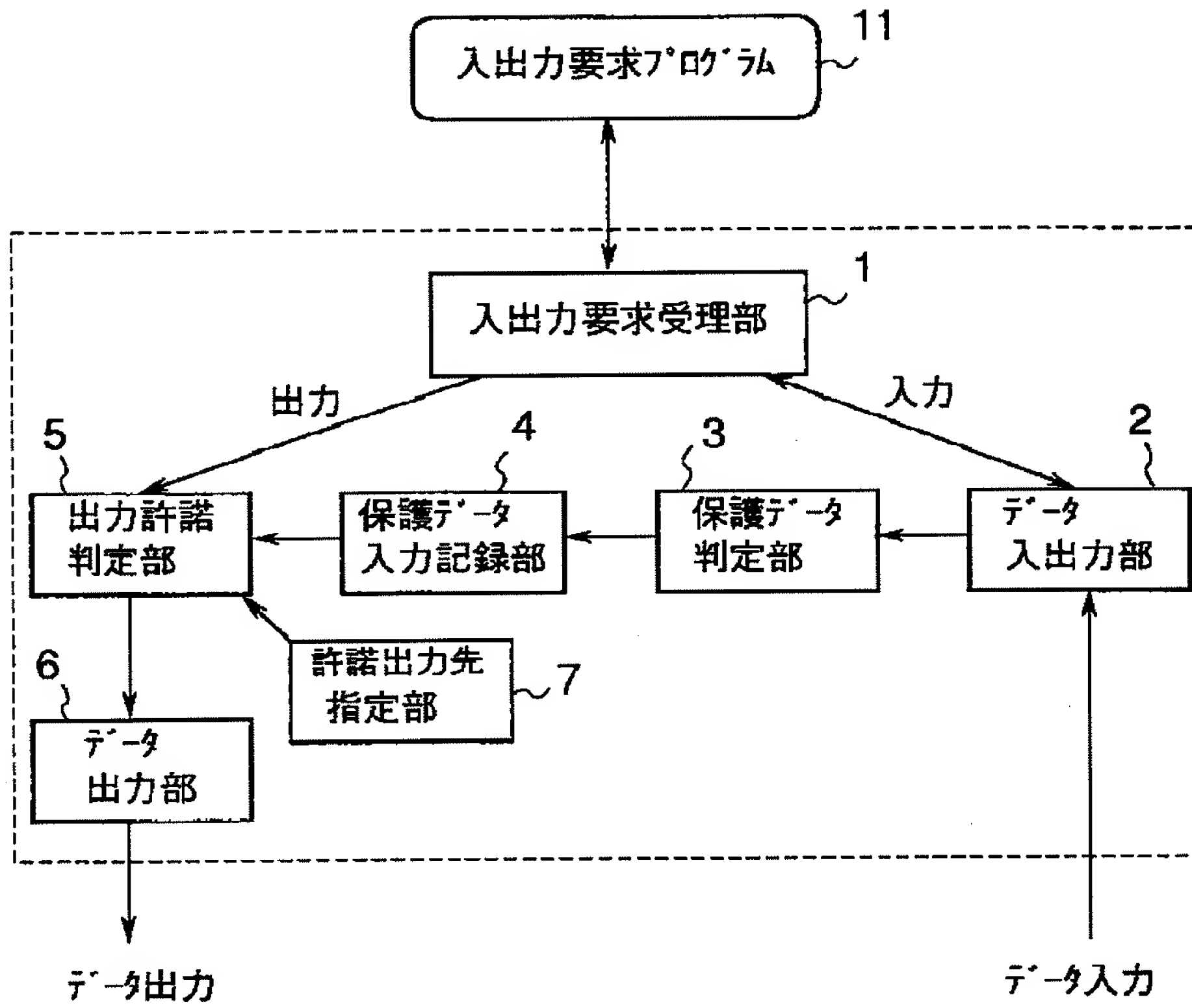
| 許諾される出力先     | データファイルID |
|--------------|-----------|
| /dev/console | all       |
| /dev/ttyφ    | 123, 65   |
| /dev/fb      | 0-127     |
| /dev/win 1   | 0-127以外   |
| ⋮            | ⋮         |

【図2】

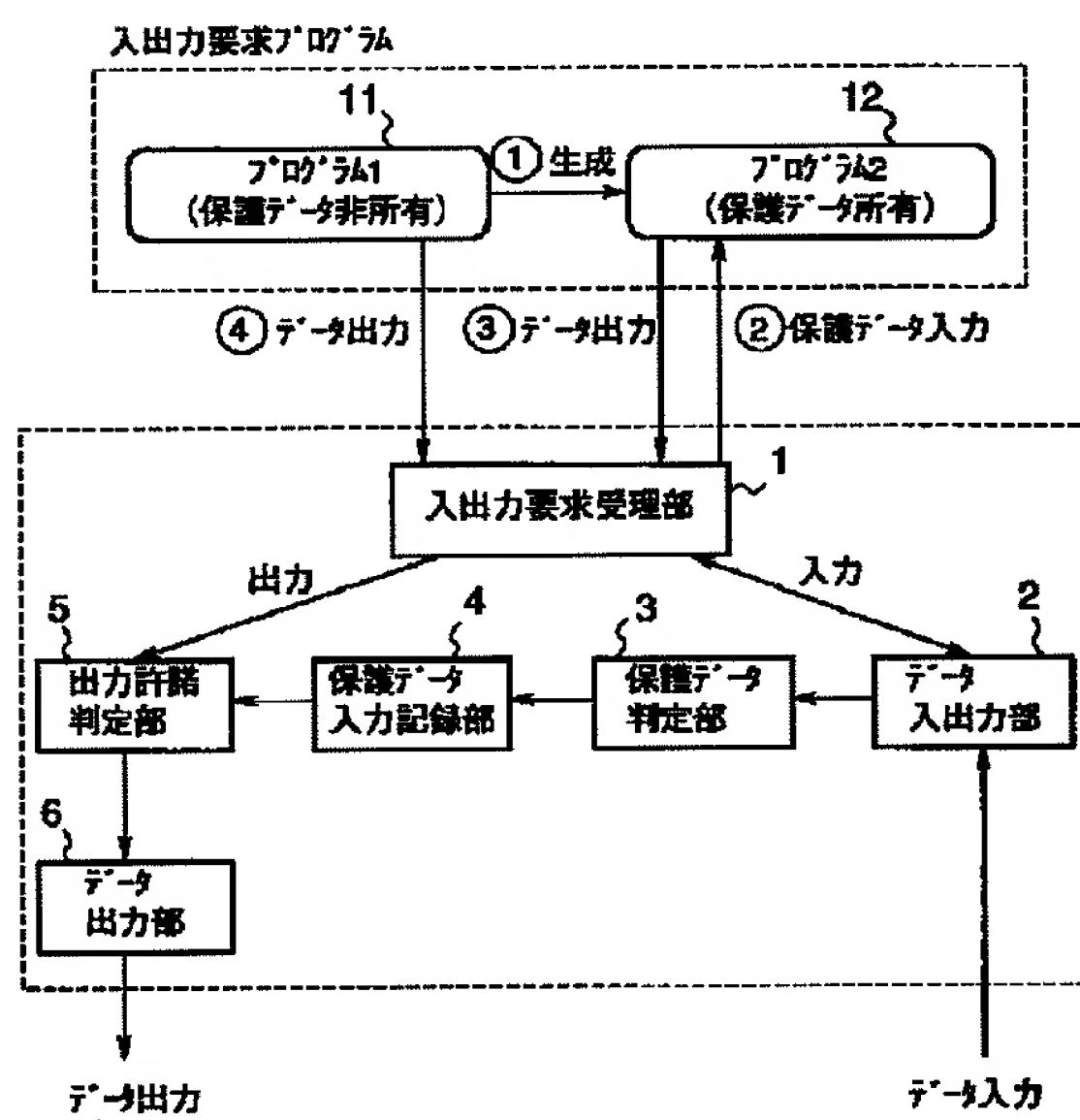




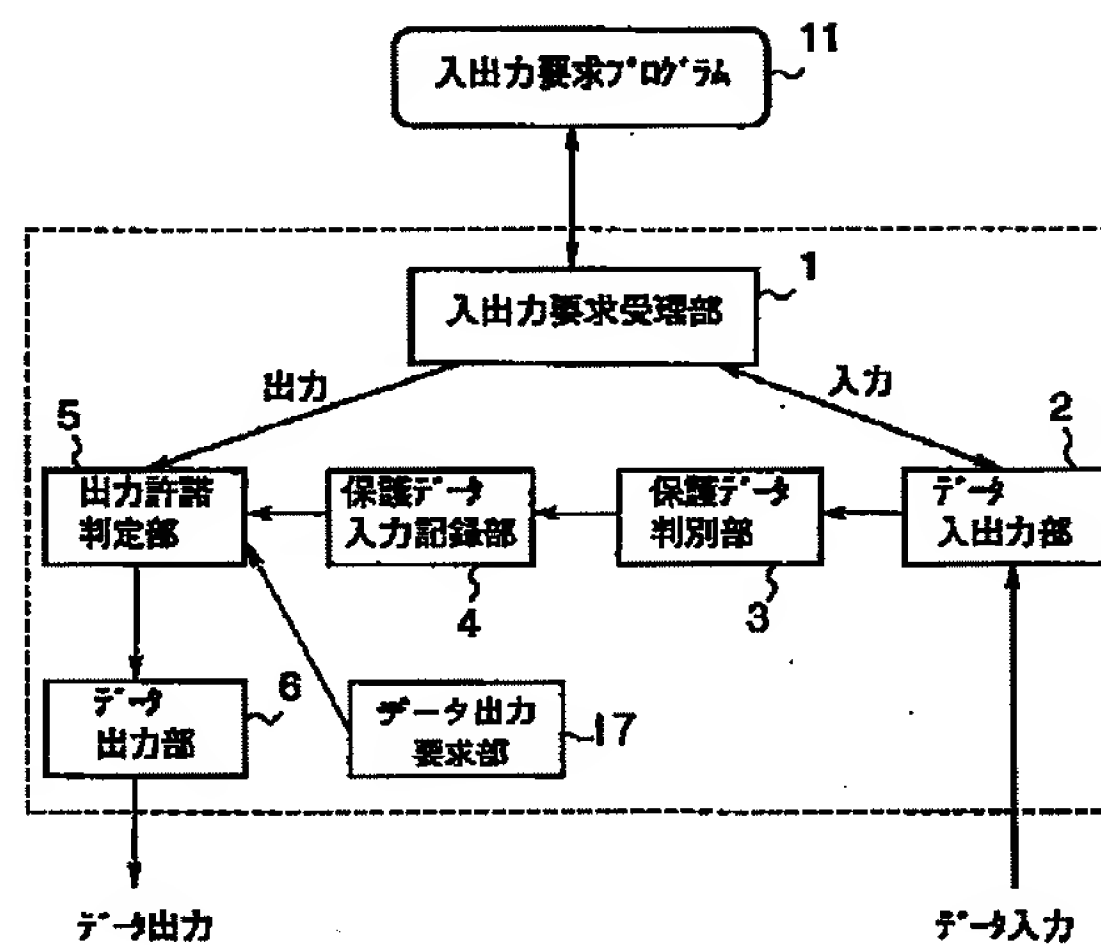
【図5】



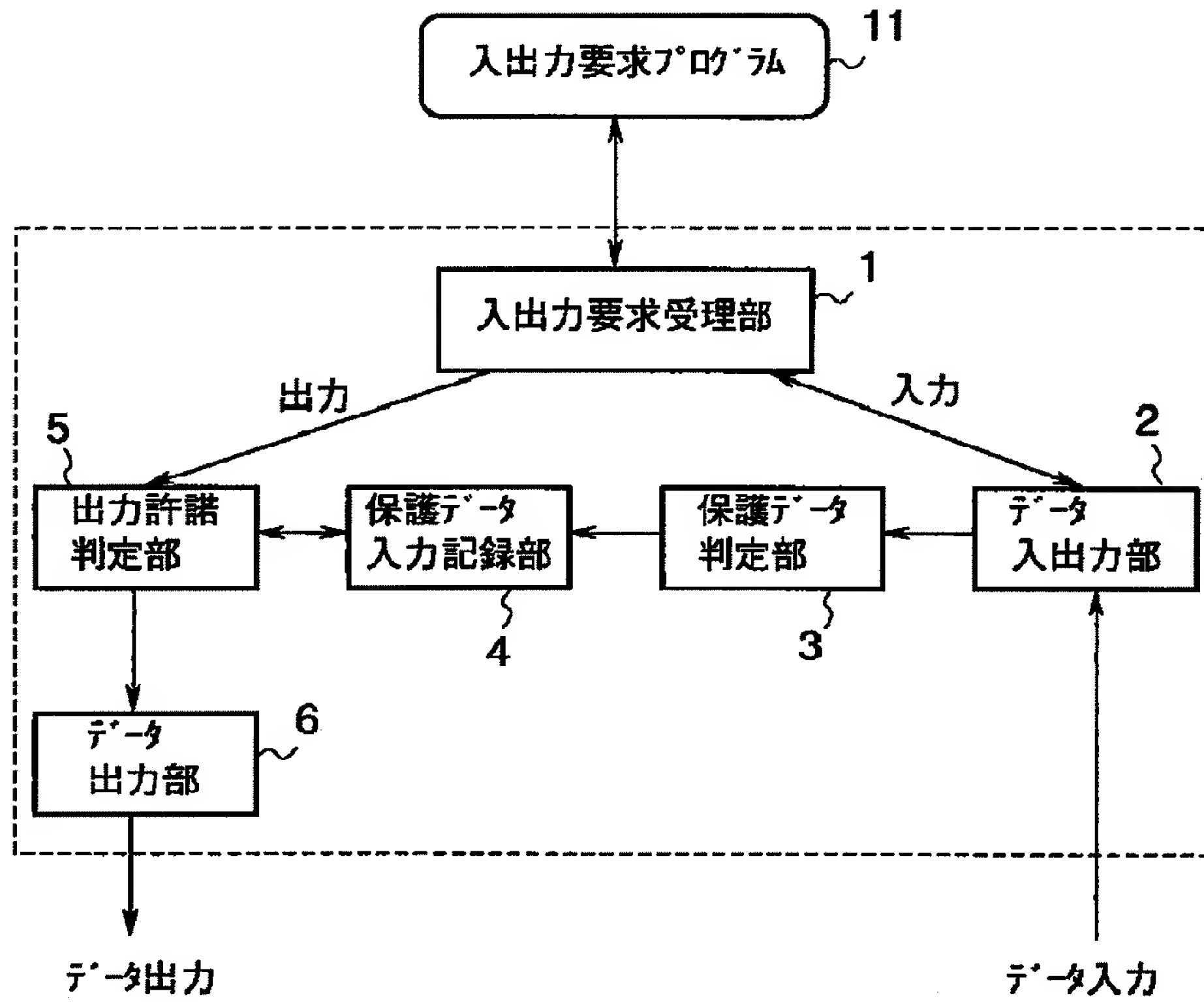
【図11】



【図12】



【図 9】



【図10】

